**PROGRAMMING AND DISCRETE MATHEMATICS (XX10190)**
**SEMESTER 2 MATHEMATICS: PROBLEM SHEET 2 – SOLUTIONS**

1. Find a generator of the group $\mathbb{F}_{31}^*$, which we know to be cyclic. You should explain why the element you have written down is a generator. How many such generators should there be?
*There should be* $\varphi(30) = 8$ *generators. One of them is* 3 *because* $3^2 = 9$, $3^3 = -4$, $3^5 = 3^2 3^3 = -5$, $3^6 = 3^3 3^3 = 16$, $3^{10} = 3^5 3^5 = -6$ *and* $3^{15} = 3^5 3^{10} = -1$, *which are all different from* 1, *so the order of* 3 *isn't be anything less than* 30. *But* 2 *doesn't work because* $2^5 = 32 = 1$ *so the order of* 2 *is* 5, *not* 30. *The other generators are* $3^a$ *with* $\mathrm{hcf}(a, 30) = 1$, *i.e.* $3^{\pm 1}$, $3^{\pm 7}$, $3^{\pm 11}$ *and* $3^{\pm 13}$, *which are* 3 *and* 21, 17 *and* 11, 13 *and* 12, *and* 24 *and* 22*: any of these instead of* 3 *is also correct.*

2. What are the finite subgroups of $K^*$ if $K = \mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$?
*The trivial group and* $\{\pm 1\}$*; the trivial group and* $\{\pm 1\}$*; and* $\{e^{2\pi i k/m},\ k = 1, \dots, m\}$ *for each* $m \in \mathbb{N}$*.*

3. Suppose that $K$ is a field of characteristic $p > 0$. Show that $(a + b)^p = a^p + b^p$ for $a,\ b \in K$.
*The binomial theorem gives this immediately once you notice that* $\binom{p}{r}$ *is divisible by* $p$ *if* $p$ *is prime and* $1 \le r \le p - 1$, *because the factor of* $p$ *in the* $p!$ *is always there.*

4. Again let $K$ be a field of characteristic $p$ and let $L = \{0, 1, 2, 3, \dots, p - 1\} \subset K$. (Here 2 is the name for the element $1 + 1 \in L$, and $3 = 2 + 1$ etc. by definition. This is a field, called the prime subfield of $K$: it is isomorphic to $\mathbb{F}_p$.) Show that taking $p$th powers in $K$ is linear over $L$: that is, if $\lambda,\ \mu \in L$ and $a,\ b \in K$ then $(\lambda a + \mu b)^p = \lambda a^p + \mu b^p$.
*As above, with the extra point that* $\lambda^p = \lambda$ *by Fermat's Little Theorem.*

GKS, 14/3/17